CLAIMS

What we claim is:

1. A system for protecting sensitive information residing in server environments, comprising at least one processing device coupled among at least one network and at least one client computer, wherein the at least one processing device:

receives at least one electronic transaction query from the at least one client computer via at least one secure channel;

evaluates the at least one electronic transaction query for sensitive data;

encrypts the sensitive data;

transfers the encrypted sensitive data among components of the server environment;

receives at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure channel;

decrypts the encrypted sensitive data in response to the at least one electronic information query; and

provides the decrypted sensitive data to the at least one third-party system via the at least one secure coupling.

2. A method for protecting sensitive information within server environments, comprising:

evaluating at least one electronic request received over at least one secure Internet channel; and

applying at least one cryptographic operation to sensitive data in response to the at least one electronic request, wherein sensitive data of the at least one electronic request is encrypted before transfer among components of the server environment, wherein encrypted sensitive data of the server environment is decrypted before transfer from the server environment.

3. The method of claim 2, further comprising determining that the at least one electronic request includes sensitive data.

4. The method of claim 2, wherein evaluating comprises identifying tags indicating that associated data is sensitive data.

5. The method of claim 2, further comprising:

determining that sensitive data in the electronic request includes at least one user password; and

applying at least one hash function to the at least one user password.

6. The method of claim 5, wherein the at least one hash function is a keyed hash function or a non-keyed hash function.

7. The method of claim 2, further comprising:

determining the at least one electronic request includes at least one cookie;

applying at least one cryptographic function or checksum to the at least one cookie.

8. The method of claim 2, wherein the at least one electronic request comprises at least one protocol over Secure Socket Layer.

9. The method of claim 2, wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords.

10. The method of claim 2, further comprising executing the at least one cryptographic operation using at least one public key.

11. The method of claim 2, wherein the at least one cryptographic operation includes at least one operation selected from a group including encryption operations, decryption operations, hash operations, keyed hash operations, and keyed hash verification.

12. The method of claim 2, wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password.

13. The method of claim 2, wherein the at least one electronic request comprises at least one encoded key identifier.

14. A method for securing sensitive information within server systems, comprising:

parsing at least one electronic request received via at least one Internet coupling;

determining that the at least one electronic request includes sensitive data;

encrypting the sensitive data; and

storing the encrypted sensitive data in at least one component of the server system.

15. The method of claim 14, further comprising:

evaluating at least one request for the encrypted sensitive data, wherein the at least one request is received via at least one coupling with at least one third-party system;

decrypting the encrypted sensitive data;

providing the decrypted sensitive data to the at least one coupling with at least one third-party system.

16. The method of claim 14, wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password.

17. A method for securing sensitive information within server systems, comprising:

evaluating at least one electronic request received from at least one third-party system via at least one proprietary channel;

determining the at least one electronic request includes a request for encrypted sensitive data and retrieving the encrypted sensitive data;

decrypting the encrypted sensitive data; and

providing the decrypted sensitive data to the at least one third-party system.

18. A system for protecting sensitive information within server systems, comprising at least one processing device coupled among at least one server site and at least one client computer and at least one network, wherein the at least one processing device evaluates at least one electronic request received via the at least one network, wherein the at least one processing device applies at least one cryptographic operation to sensitive data in response to the at least one electronic request, wherein sensitive data of the at least one electronic request is encrypted prior to transfer among components of the at least one server system, wherein encrypted sensitive data of the at least one server system is decrypted prior to transfer among the at least one network.

19. The system of claim 18, wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags indicating that associated data is the sensitive data.

20. The system of claim 18, wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags specified by at least one system administrator that associated data is the sensitive data.

21. The system of claim 18, wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords.

22. The system of claim 18, wherein the at least one cryptographic operation includes at least one operation selected from a group including encryption operations, decryption operations, hash operations, and keyed hash operations.

23. A cryptographic appliance for securing sensitive information within a server system, comprising:

at least one processing device coupled among at least one server system and at least one Internet coupling to evaluate at least one received electronic request, wherein the at least one processing device;

determines when the at least one received electronic request includes sensitive data;

encrypts the sensitive data; and

transfers the encrypted sensitive data among at least one component of the at least one server system.

24. The cryptographic appliance of claim 23, wherein the at least one processing device:

evaluates at least one request for the encrypted sensitive data received via at least one coupling with at least one third-party system;

decrypts the encrypted sensitive data; and

transfers the decrypted sensitive data to the at least one third-party system.

25. A cryptographic appliance for securing sensitive information within a server system, comprising:

at least one processing device coupled among at least one server system and at least one third-party system, wherein the at least one processing device:

receives at least one electronic request for encrypted sensitive information;

retrieves the encrypted sensitive information

decrypts the encrypted sensitive information; and

provides the decrypted sensitive data to the at least one third-party system.

26. A computer readable medium containing executable instructions which, when executed in a processing system, protects sensitive information within server environments by:

evaluating at least one electronic request received over at least one network coupling; and

applying at least one cryptographic operation to sensitive data in response to the at least one electronic request, wherein sensitive data of the at least one electronic request is encrypted prior to transfer among components of the server environments, wherein encrypted sensitive data of the server environments is decrypted prior to transfer among the at least one network coupling.

27. An electromagnetic medium containing executable instructions which, when executed in a processing system, protects sensitive information within server environments by:

evaluating at least one electronic request received over at least one network coupling; and

applying at least one cryptographic operation to sensitive data in response to the at least one electronic request, wherein sensitive data of the at least one electronic request is encrypted prior to transfer among components of the server environments, wherein encrypted sensitive data of the server environments is decrypted prior to transfer among the at least one network coupling.

28. A device for protecting sensitive information within server environments, comprising:

means for receiving at least one electronic transaction query from the at least one client computer via at least one secure coupling;

means for evaluating the at least one electronic transaction query for sensitive data;

means for encrypting detected sensitive data;

means for transferring the encrypted sensitive data among components of the server environment;

means for receiving at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure coupling;

means for decrypting the encrypted sensitive data in response to the at least one electronic information query; and

means for transferring the decrypted sensitive data to the at least one third-party system via the at least one secure coupling.